Journal of Combinatorial Theory, Series A **83**, 79–93 (1998)
Article No. TA972864

Divisibility of Codes Meeting the Griesmer Bound*

Harold N. Ward

Department of Mathematics, University of Virginia, Charlottesville, Virginia 22903

Communicated by Vera Pless

Received November 10, 1997

We prove that if a linear code over $GF(p)$, p a prime, meets the Griesmer bound, then if p^e divides the minimum weight, p^e divides all word weights. We present some illustrative applications of this result. © 1998 Academic Press

1. INTRODUCTION

The familiar Griesmer bound says that for an $[n, k, d]$ code C over $GF(q)$,

$$n \geqslant \sum_{i=0}^{k-1} \lceil d/q^i \rceil.$$

The brackets of "$[n, k, d]$" signal that C is linear, and n is the length, k the dimension, and d the minimum weight of C. The bound was proved by Griesmer in 1960 for $q = 2$ and generalized by Solomon and Stiffler in 1965. Over the years, much effort has gone into constructing codes meeting the bound or showing, for selected parameter values, that they do not exist. This effort is part of the more comprehensive program of finding optimal linear codes over $GF(q)$, those having the smallest n for given k and d. The recent paper [14] of Hill provides a thorough survey of this research and a sizeable bibliography. We shall abbreviate the right side of the bound by $g_q(k, d)$ and call a code meeting the bound a Griesmer code.

A divisor of a linear code is an integer dividing the weights of all its words, and a code is called divisible if it has a divisor larger than 1 [20]. Optimal codes are often divisible, and Dodunekov and Manev showed that for a binary code meeting the Griesmer bound, the power of 2 dividing the

* This work was partially supported by NSA Grant MDA904-95-H-1040. E-mail: hnw@virginia.edu.

0097-3165/98 $25.00

minimum weight is a divisor of the code [9]. The purpose of the present paper is to prove and apply the following generalization of their result.

THEOREM 1. *Let C be an $[n, k, d]$ code over $GF(p)$, p a prime, meeting the Griesmer bound. If $p^e \mid d$, then p^e is a divisor of C.*

2. CODES OF TYPE *BV*

There is evidence more substantial than just scattered weight distributions that certain Griesmer codes are divisible. Following Section 2 of [14], we shall outline the construction of codes of type BV meeting the Griesmer bound. The labeling honors Belov, who produced the codes in the binary case (as cited in [14]); the generalizaiton to arbitrary field sizes was effected by Dodunekov [7]. These codes are plentiful enough to show that for given k and q, Griesmer codes exist for large enough d (Corollary 2.14 of [14]; the binary case of this result was proved by Baumert and McEliece [2], and the general case by Dodunekov [6]).

Searching for an $[n, k, d]$ Griesmer code over $GF(q)$, write $d = sq^{k-1} - \sum_{i=1}^{k-1} a_i q^{i-1}$, where $s = \lceil d/q^{k-1} \rceil$ and $0 \leqslant a_i \leqslant q-1$. Let V be a k-dimensional vector space over $GF(q)$. The set $P(V)$ of 1-dimensional subspaces of V is the point set of the projective space associated with V. The subsets $P(U)$, for U a subspace of V, are construed as the projective subspaces of $P(V)$. If $\dim U = \ell$, then $|P(U)| = (q^\ell - 1)/(q-1)$, which we shall abbreviate by the Gaussian coefficient $\begin{bmatrix} \ell \\ 1 \end{bmatrix}$. Any nonzero vector is said to represent the 1-dimensional subspace it spans.

Let S be a multiset of members of V such that every member of $P(V)$ is represented by s members of S. Suppose that we can select subspaces of V in such a way that there are a_i subspaces of dimension i and that no point in the corresponding projective subspaces appears more than s times. Remove from S vectors representing the points of these projective subspaces, one for each appearance, to create the set S'. Then

$$|S'| = n = s \begin{bmatrix} k \\ 1 \end{bmatrix} - \sum_{i=1}^{k-1} a_i \begin{bmatrix} i \\ 1 \end{bmatrix}$$

Now create the code C of length n by ordering the members of S' in some way and assigning to each linear functional λ of V the word $c(\lambda)$ whose components are the values $\lambda(v)$, $v \in S'$. The list of components of $c(\lambda)$ is obtained by taking the list of all the values $\lambda(v)$, $v \in S$, and deleting the $\lambda(u)$ for which u represents a point of $P(U)$ for one of the selected subspaces U. If $\lambda(U) = 0$, the deleted values for $P(U)$ are all 0. But if $\lambda(U) \neq 0$

and dim $U=i$, $\begin{bmatrix} i \\ 1 \end{bmatrix} - \begin{bmatrix} i-1 \\ 1 \end{bmatrix} = q^{i-1}$ of the deleted values are nonzero. Consequently, if $\lambda \neq 0$, the weight $w(c(\lambda))$ is

$$w(c(\lambda)) = sq^{k-1} - \sum q^{\dim U - 1},$$

the summation over the selected subspaces U for which $\lambda(U) \neq 0$. The first term is the number of v in S for which $\lambda(v) \neq 0$.

As shown in [14], C is indeed an $[n, k, d]$ Griesmer code over $GF(q)$. What we wish to draw from the construction is this:

PROPOSITION 2. *Let C be an $[n, k, d]$ code of type BV over $GF(q)$. Suppose that $q^e \mid d$. Then q^e is a divisor of C.*

Proof. If $q^e \mid d$, then $e \leqslant i-1$ if $a_i \neq 0$. Thus $q^e \mid q^{\dim U - 1}$ for any of the selected subspaces, U, and so $q^e \mid w(c(\lambda))$ for $\lambda \neq 0$. ∎

Theorem 1 does not seem to generalize to the extent this proposition suggests. For example, the famous hexacode, a $[6, 3, 4]$ code over $GF(4)$, is a Griesmer code divisible by 2, but not 4. (There is, in fact, a generalization of Theorem 1 for $GF(4)$: if $4^e \mid d$, d the minimum weight of a Griesmer code over $GF(4)$, then 2^e divides the code. But examples indicate that something stronger should be true.)

3. PRELIMINARIES

For a code C, let $A_i(C)$ be the number of words of weight i in C, and $B_i(C)$ the number of words of weight i in the dual of C. We shall refer to a linear code of length n and dimension k as an $[n, k]$ code when the minimum weight does not need indicating, and we shall just write A_i and B_i when the code is clear. We shall invoke the MacWilliams identities in the following form, for an $[n, k]$ code over $GF(q)$ ([18, Lemma 2.9(ii)]; such special forms of the identities are also given in [19]).

$$\sum_{i=m}^{n} \binom{i}{m} A_i = q^{k-m} \sum_{j=0}^{m} \binom{n-j}{m-j} (-1)^j (q-1)^{m-j} B_j.$$

These are valid for $0 \leqslant m \leqslant n$.

For a word c, let $\mathrm{supp}(c)$ be the set of places (coordinate locations) where c has a nonzero entry, and for a code C, let $n(C) = |\bigcup_{c \in C} \mathrm{supp}(c)|$, the effective length of C.

Since $n(C) = n - B_1(C)/(q-1)$ for a code of length n over $GF(q)$, $m=1$ in the identities implies:

LEMMA 3. *Let C be an $[n, k]$ code over $GF(q)$. Then*

$$\sum_{c \in C} w(c) = \sum_{i=0}^{n} iA_i(C) = q^{k-1}(q-1)\, n(C).$$

The next proposition has several uses.

PROPOSITION 4. *Let C be an $[n, k]$ code over $GF(q)$ with $n(C) = n$. Let D be an ℓ-dimensional subcode. Then there is a supplementary subcode D' (one with $D \cap D' = 0$ and $D + D' = C$) for which*

$$n(D') \leqslant n - \lceil n(D)/q^{k-\ell} \rceil.$$

Proof. The supplements D' of D are spanned by preimages of a fixed basis of C/D. Each of the $k-\ell$ basis elements has q^{ℓ} preimages, so there are $q^{\ell(k-\ell)}$ supplements. If $c \in C \backslash D$ and we select the basis to make c one of the preimages, we find that c is in $q^{\ell(k-\ell-1)}$ of the supplements.

It follows that

$$\sum_{D'} \left(\sum_{i=0}^{n} iA_i(D') \right) = q^{\ell(k-\ell-1)} \left\{ \sum_{i=0}^{n} iA_i(C) - \sum_{i=0}^{n} iA_i(D) \right\}$$

the left sum over all supplements D' of D. Invoking Lemma 3 several times, we obtain:

$$\sum_{D'} n(D')\, q^{k-\ell-1}(q-1) = q^{\ell(k-\ell-1)} \{ nq^{k-1}(q-1) - n(D)\, q^{\ell-1}(q-1) \},$$

whereupon

$$\sum_{D'} n(D') = q^{\ell(k-\ell)} \{ n - n(D)/q^{k-\ell} \}.$$

Consequently, the average value of $n(D')$ is the second factor on the right. Since $n(D')$ is an integer, we have that for some D',

$$n(D') \leqslant n - \lceil n(D)/q^{k-\ell} \rceil. \quad \blacksquare$$

One can now prove the Griesmer bound by induction on k, taking $D = \langle c \rangle$, with c of minimum weight. In the same vein, we have:

COROLLARY 5. *Suppose C is an $[n, k, d]$ Griesmer code over $GF(q)$, and $q^{k-1} \mid d$. Then C is a constant weight code: all nonzero words have weight d.*

Proof. Again, take $D = \langle c \rangle$, $c \neq 0$; $n(D) = w(c) \geqslant d$. Then for some supplement D',

$$\lceil w(c)/q^{k-1} \rceil \leqslant n - n(D').$$

The right side is at most $g_q(k, d) - g_q(k-1, d) = \lceil d/q^{k-1} \rceil = d/q^{k-1}$. Thus $w(c) \leqslant d$, and so $w(c) = d$. ∎

Constant weight linear codes are equivalent to replicated (concatenated) Hamming duals [3, 22].

The next corollary is a theorem of Dodunekov [8]:

COROLLARY 6. *Let C be an $[n, k, d]$ code over $GF(q)$ with $n = t + g_q(k, d)$. Then C has a basis of words whose weights are at most $t + d$.*

Proof. For $k = 1$, the result is evident, and we can induct on k. Take $c \in C$ with $w(c) = d$, and let D' be a supplement to $\langle c \rangle$, as before, with

$$n(D') \leqslant n - \left\lceil \frac{d}{q^{k-1}} \right\rceil.$$

If d' is the minimum weight of D', then

$$g_q(k-1, d') \leqslant n(D') \leqslant n - \left\lceil \frac{d}{q^{k-1}} \right\rceil = t + g_q(k-1, d).$$

If $t' + d' = t + d$, the last quantity is

$$\begin{aligned} t + d + \sum_{i=1}^{k-2} \lceil d/q^i \rceil &= t' + d' + \sum_{i=1}^{k-2} \lceil d/q^i \rceil \\ &\leqslant t' + d' + \sum_{i=1}^{k-2} \lceil d'/q^i \rceil \\ &= t' + g_q(k-1, d'). \end{aligned}$$

Thus $n(D') = t'' + g_q(k-1, d')$, with $t'' \leqslant t'$. By induction, D' has a basis of words of weights at most $t'' + d' \leqslant t + d$, and adjoining c gives the required basis for C. ∎

In particular, $t = 0$ shows that a Griesmer code has a basis of minimum weight words.

Consider now divisible codes. If Δ is a divisor of a code and Δ is relatively prime to the alphabet size, the code is equivalent to a Δ-fold replicated code (one obtained by repeating each digit of a shorter code Δ times), possibly with some additional 0 coordinates ([20], Theorem 1). Thus the more interesting situation is that of linear codes over $GF(q)$, q a power of the prime p, having divisors that are powers of p. The exponent

e of the highest power p^e that is a divisor of such a code is called the exponent of the code.

A technique for determining the exponent of a code from properties of a spanning set was developed in [21]. Let $\mathbf{Z}_p$ be the ring of p-adic integers, with residue class field $\mathbf{Z}_p/p\mathbf{Z}_p = GF(p)$. Among its units, Z_p contains the $(p-1)$-st roots of unity, and they and 0 can be taken as preimages of the members of $GF(p)$. Thus for $\alpha \in GF(p)$, let $T(\alpha)$ be the preimage of α that is either 0 or one of the $(p-1)$-st roots of unity; $T(\alpha)$ is called the Teichmüller representative of α. For a word $a = (\alpha_1, ..., \alpha_n)$, with $\alpha_i \in GF(p)$, let $T(a) = (T(\alpha_1), ..., T(\alpha_n))$, the Teichmüller lift of a.

If R is any commutative ring, and $a_i \in R^n$ for $i = 1, ..., r$, let the component-wise product of $a_1, ..., a_r$ be denoted by $a_1 \cdots a_r$. Then for $a \in R^n$, let $\sigma(a)$ be the sum of the components of a. The r-fold dot product of $a_1, ..., a_r$ is $\sigma(a_1 \cdots a_r)$. It is also called the standard form of degree r, or the standard r-form, evaluated at $a_1, ..., a_r$.

The divisibility criterion we shall invoke is a special case of Theorem 5.3 of [21]:

THEOREM 7. *Let C be a linear code over $GF(p)$, p a prime, and let S be a spanning set of C. Then p^e is a divisor of C if and only if*

$$p^{e+1-m} \mid \sigma(T(c_1) \cdots T(c_{m(p-1)}))$$

for all $m (\leqslant e)$ and all choices of $c_1, ..., c_{m(p-1)}$ in S, duplications allowed.

Since the entries in the Teichmüller lifts are 0's or $(p-1)$-st roots of unity, one may assume no factor occurs more than $p-1$ times, because a reduction modulo $p-1$ to a positive remainder results in a product of lower degree.

4. PROOF OF THEOREM 1

Let C be an $[n, k, d]$ Griesmer code over $GF(p)$, p a prime, for which $p^e \mid d$, $e \geqslant 1$. We need to show that p^e is a divisor of C, and we shall use induction on k and e. Let C_1 be a Griesmer subcode of C of codimension 1: $n(C_1) = g_p(k-1, d)$. C_1 can be created as a supplement of $\langle c \rangle$, $w(c) = d$, promised by Proposition 4 (such a C_1 also arises in the usual step-by-step proof of the Griesmer bound). Since C is spanned by minimum weight words, there is a codeword $a \notin C_1$ with $w(a) = d$. We shall apply Theorem 7 to the set $S = \{a\} \cup C_1$. Let $A = T(a)$, and let $P(r)$ stand for a product of the Teichmüller lifts of r arbitrary members of C_1. Then what we need to show is that

$$p^{e+1-m} \mid \sigma(A^t P((p-1)(m-1)-t))$$

for all choices of the ingredients from C_1, all $m \leqslant e$, and all $t \leqslant p-1$.

The residual code of C with respect to a word $b \in C$ is the code obtained by puncturing C at the support of b (see Section 2 of [14]). Let $\mathrm{res}(C, b)$ be this code and let $\mathrm{res}(c, b)$ be the image of $c \in C$ in it. Then $\mathrm{res}(C, a)$ is an $[n-d, k-1, d/p]$ Griesmer code, and by induction it is divisible by p^{e-1}. The subcode C_1 is divisible by p^e, also by induction. It follows that for $c \in C_1$, the projection of c onto the support of a has weight divisible by p^{e-1}, since that projection is obtained by removing the entries in $\mathrm{res}(c, a)$. This projection, or more properly, the projection extended to a word of length n by 0's outside $\mathrm{supp}(a)$, can be written as $a^{p-1}c$. For a^{p-1} has entries 1 on $\mathrm{supp}(a)$ and 0's elsewhere. By Theorem 7 (with all of C_1 as the spanning set!) we have

$$p^{e+1-m} \mid \sigma(A^{p-1}P((p-1)(m-1))),$$

since $e+1-m = (e-1)+1-(m-1)$. In other words, the required divisibility of form values is correct for $t = p-1$. Notice that all we need about a is that $w(a) = d$ and $a \notin C_1$. Of course, the divisibility is trivially correct for $m = e+1$. Thus given t and m, we may assume for all $t' > t$, or all $m' > m$ when $t' = t$, that

$$p^{e+1-m'} \mid \sigma(A^{t'}P((p-1)\, m' - t')),$$

again for all ingredients from C_1 and for all a with $w(a) = d$ and $a \notin C_1$.

Now fix a (so restricted). Because a has minimum weight, the map $C_1 \to \mathrm{res}(C, a)$ is a bijection. In C_1, take the preimage of a basis of minimum weight words of $\mathrm{res}(C, a)$ (that weight is d/p). If b is a nonzero scalar multiple of one of the preimages, $n(\langle a, b\rangle) = d + d/p$. As this is $g_p(2, d)$, Corollary 5 implies that $\langle a, b\rangle$ is a constant weight code. So $w(b) = w(a+\alpha b) = d$ for all $\alpha \in GF(p)$. Thus

$$p^{e+1-m} \mid \sigma(T(a+\alpha b)^{t+1}\, P((p-1)\, m - t - 1)).$$

We need the expansion formula for $T(x+y)$ that is presented in Proposition 2.2 of [21], along with the p-power divisibilities of the coefficients from Theorem 3.2 of that paper.

PROPOSITION 8. *Let $x, y \in GF(p)^n$, and let $T(x) = X$, $T(y) = Y$. Then for $1 \leqslant r \leqslant p-1$,*

$$T(x+y)^r = X^r + Y^r + \sum_{i=1}^{r-1} c(r, i)\, X^{r-i}Y^i + \sum_{i=r}^{p-1} c(r, i)\, X^{p-1+r-i}Y^i,$$

where $p \nmid c(r, i)$ *for* $1 \leqslant i \leqslant r-1$, *but* $p \mid c(r, i)$ (*and in fact* $p^2 \nmid c(r, i)$) *for* $r \leqslant i \leqslant p-1$.

Let $B = T(b)$ and abbreviate $P((p-1)m-t-1)$ to P. Let α stand for $T(\alpha)$ (they are both 0 or $(p-1)$-st roots of unity!). Then the form divisibility above, with the expansion, becomes

$$p^{e+1-m} \mid \sigma(A^{t+1}P) + \alpha^{t+1}\sigma(B^{t+1}P) + \sum_{i=1}^{t} \alpha^i c(t+1, i)\, \sigma(A^{t+1-i}B^iP) + \sum_{i=t+1}^{p-1} \alpha^i c(t+1, i)\, \sigma(A^{p+t-i}B^iP).$$

For the divisibility of the individual terms, we have $p^{e+1-m} \mid \sigma(A^{t+1}P)$ by assumption. $B^{t+1}P$ just involves C_1, which is divisible by p^e, so $p^{e+1-m} \mid \sigma(B^{t+1}P)$. In the second sum, $p+t-i \geqslant t+1$, so the divisibility appropriate to the degree applies. That degree is $p+t-i+i+(p-1)m-t-1 = (p-1)(m+1)$. Moreover, $p \mid c(t+1, i)$ for these i. Thus p^{e+1-m} divides the whole term for the index i.

We thus find that p^{e+1-m} divides the first sum, which we may write as $c(\alpha)\, p^{e+1-m}$. That is,

$$\sum_{i=1}^{t} \alpha^i c(t+1, i)\, \sigma(A^{t+1-i}B^iP) = c(\alpha)\, p^{e+1-m}.$$

Select t different nonzero values of α and solve the equations for the $c(t+1, i)\, \sigma(A^{t+1-i}B^iP)$. The determinant involved is Vandermonde and a unit in $\mathbf{Z}_p$, as its image in $GF(p)$ is not 0. As $p \nmid c(t+1, i)$, we infer that

$$p^{e+1-m} \mid \sigma(A^{t+1-i}B^iP)$$

for $1 \leqslant i \leqslant t$, and in particular, $p^{e+1-m} \mid \sigma(A^tBP)$.

Let $x \in C_1$, with $T(x) = X$. We wish to show that $p^{e+1-m} \mid \sigma(A^tXP)$. Express x as a linear combination of the preimage basis members, and let ℓ be the number of nonzero terms. We have just shown the required divisibility when $\ell = 1$. Inducting on ℓ, write $x = b + y$, where b is a scalar multiple of a basis element and y is a combination of $\ell - 1$ basis elements. With $T(y) = Y$, expand $T(b+y)$ by Theorem 7 to see that

$$\sigma(A^tXP) = \sigma(A^tBP) + \sigma(A^tYP) + \sum_{i=1}^{p-1} c(1, i)\, \sigma(A^tB^{p-i}Y^iP).$$

Once again, the first two terms are divisible by p^{e+1-m} by assumption. In the terms of the sum, the degree of the form is $t+p-i+i+(p-1)m-t-1 = (p-1)(m+1)$, so the form values are assumed divisible by

$p^{e+1-(m+1)}$ from the larger degree. As $p \mid c(1, i)$, p^{e+1-m} divides the whole term. Thus $p^{e+1-m} \mid \sigma(A^t XP)$. As x is arbitrary in C, we now have

$$p^{e+1-m} \mid \sigma(A^t P((p-1)\, m - t))$$

in the generality required for members of C_1.

Thus the divisibility of Theorem 1 is established.

5. EXAMPLES

We first recall some results from [16].

LEMMA 9 ([16], Lemma 2.4). *Let a and b be linearly independent words in a code over $GF(q)$. Then*

$$w(a) + \sum_{\alpha \in GF(q)} w(\alpha a + b) = qn(\langle a, b \rangle).$$

Proof. This follows from Lemma 3 with $k = 2$ on taking scalar multiples into account. ∎

If a and b are in an $[n, k, d]$ code, then as $w(\alpha a + b) \geqslant d$ and $n(\langle a, b \rangle) \leqslant n$, we get $w(a) \leqslant q(n-d)$. And by the same token, $w(a) + w(b) \leqslant qn - (q-1)\, d$. These facts lead to items in Corollary 2.7 of [16]:

LEMMA 10. *Let C be an $[n, k, d]$ code over $GF(q)$ with $k \geqslant 2$. Then*

(1) $A_i(C) = 0$ *if* $i > q(n-d)$;

(2) $A_i(C) = 0$ *or* $q-1$ *if* $i > (qn - (q-1)\, d)/2$;

(3) *if* $A_i(C) \neq 0$ *for some* i, *then* $A_j(C) = 0$ *for* $j \neq i$ *and* $j > qn - (q-1)\, d - i$.

LEMMA 11 ([16], Lemma 2.13). *Let C be an $[n, k, d]$ code over $GF(q)$, and let $a \in C$, $a \neq 0$. Then if $w = w(a) < qd/(q-1)$, $\mathrm{res}(C, a)$ is an $[n-w, k-1, d']$ code with $d' \geqslant d - w + \lceil w/q \rceil$.*

LEMMA 12 ([16], Theorem 2.16). *Suppose C is an $[n, k, d]$ Griesmer code over $GF(q)$, and that $d \leqslant q^{k+1-j}$ for some $j > 0$. Then $B_j(C) = 0$.*

We also have this result on the divisibility of residuals.

LEMMA 13. *Let C be a linear code over $GF(q)$ that is divisible by Δ. Then for any $a \in C$, $\mathrm{res}(C, a)$ is divisible by $\Delta / gcd(\Delta, q)$.*

Proof. Take $a \neq 0$ and $b \notin \langle a \rangle$. All the terms on the left of the equation in Lemma 9 are divisible by Δ, so that $\Delta \mid qn(\langle a, b \rangle)$. Since $w(\mathrm{res}(b, a)) = n(\langle a, b \rangle) - w(a)$ and $\Delta | w(a)$, we have $\Delta / gcd(\Delta, q) \mid w(\mathrm{res}(b, a))$. ∎

The first example is the computation of the weight distribution of a hypothetical [149, 5, 99] Griesmer code over $GF(3)$. In the compilation of optimal ternary codes of dimension 5 in [16], the value of n for $d = 99$ was narrowed to 149 or 150. It has since been shown (by Brouwer and van Eupen [5] and Landgev [17]) that the Griesmer code does not exist. The purposes of giving the example are to show how Theorem 1 expedites the computation and to display some standard arguments.

Let C be a [149, 5, 99] Griesmer code over $GF(3)$. One has $B_1 = 0$ for any Griesmer code; Lemma 12 provides no more information. By Theorem 1, the possible word weights are the multiples of 9 from 99 to 144. Lemma 11 applies to all these weights, since the bound there is $3 \cdot 99/2 = 148.5$. The residuals by word weights are:

Weight	Residual
144	[5, 4, 3]
135	[14, 4, 9]
126	[23, 4, 15]
117	[32, 4, 21]
108	[41, 4, 27]
99	[50, 4, 33]

(The minimum weights given are the d' of Lemma 11.) Weight 144 is ruled out because $g_3(4, 3) = 6$, and 135 and 126 are excluded by the entries for $d = 9$ and 15 in Table 2 of [16]. Had we not invoked Theorem 1, weights 109, 110, 111, 113, 114, 122, 123, and 149 would have survived this initial scrutiny.

Our main goal is to show that $A_{117}(C) = 0$. To that end, suppose $A_{117}(C) > 0$ and consider $C' = \mathrm{res}(C, a)$ for a word a with $w(a) = 117$. C' is a [32, 4, 21] Griesmer code whose possible word weights are 21, 24, 27, and 30 (by Theorem 1 or Lemma 13). Since $3d/2 = 31.5$ here, Lemma 11 again applies to all weights. The residuals are:

Weight	Residual
30	[2, 3, 1]
27	[5, 3, 3]
24	[8, 3, 5]
21	[11, 3, 7]

Weight 30 is out immediately, and 27 is excluded by Theorem 3.1 of [16]. The weight enumerator comes out to be $1+64z^{21}+16z^{24}$ from the MacWilliams identities for $m=0$ and 1, with $B_0=1$, $B_1=0$. One has $B_2(C')=0$ (by Lemma 12, in fact).

Consider how the words b of C outside $\langle a\rangle$ distribute according to $w(\mathrm{res}(b,a))$. Lemma 9 implies

$$3(w(a)+w(\mathrm{res}(b,a)))=3n(\langle a,b\rangle)$$
$$=w(a)+w(b)+w(a+b)+w(2a+b).$$

That is, $3w(\mathrm{res}(b,a))+2w(a)=w(b)+w(a+b)+w(2a+b)$; or with $w(a)=117$,

$$3w(\mathrm{res}(b,a))+234=w(b)+w(a+b)+w(2a+b).$$

If $w(b)=117$, the right side is at least $117+99+99=315$, and $w(\mathrm{res}(b,a))\geqslant 27$. As that is not possible, we conclude that $A_{117}(C)=2$.

This is enough to determine the weight distribution of C by the MacWilliams identities, and we get

$$A_0=1,\qquad A_{99}=224,\qquad A_{108}=16,\qquad A_{117}=2.$$

We also find $B_2=68$. Referring to words by their weights, we have no 2's of $C^\perp$ with support disjoint from $\mathrm{supp}(a)$, since $B_2(C')=0$. The support of a 2 in $C^\perp$ cannot meet $\mathrm{supp}(a)$ in just one place, so all the 2's of $C^\perp$ have supports in $\mathrm{supp}(a)$. Two of these supports cannot meet in just one place; for if C were shortened at such a place, three coordinates would become 0. The shortened code would be a $[146,4,99]$ code violating the Griesmer bound.

Now scale the coordinates to make the nonzero entries of a all 1's, and picture a generator matrix for C with a as top row. Look at the columns in $\mathrm{supp}(a)$. Pairs of duplicated columns correspond to the supports of the 2's in $C^\perp$. Thus there are $68/2=34$ such pairs, and $117-68=49$ single columns. So we see $34+49=83$ different columns, and yet only 81 are available!

Hence, in fact, $A_{117}(C)=0$. The weight distribution (the MacWilliams identities again) is then

$$A_0=1,\qquad A_{99}=222,\qquad A_{108}=20,$$

as in [16].

The next example is another proof of the theorem of Hamada, Helleseth, and Ytrehus that there is no $[51,5,33]$ Griesmer code over $GF(3)$ [12].

Along with the results of [16], this means the optimal code for $k = 5$ and $d = 33$ has $n = 52$.

The initial steps are analogous to those in the first example: we let C be a hypothetical [51, 5, 33] code. Then we use Theorem 1 and Lemma 11 to limit the word weights and the corresponding residuals.

Weight	Residual
48	[3, 4, 1]
45	[6, 4, 3]
42	[9, 4, 5]
39	[12, 4, 7]
36	[15, 4, 9]
33	[18, 4, 11]

Weight 48 is excluded outright, and 45 and 39 are out by the entries for $d = 3$ and 7 of Table 2 of [16]. (This time the extra weights without divisibility would have been 41 and 50.)

Lemma 10 applies, with $3n - 2d = 87$, to show that $A_{51} = 0$ or 2 and that if $A_{51} = 2$, then $A_{42} = 0$. Lemma 12 implies $B_1 = B_2 = 0$. Now one can use the MacWilliams identities; but they do not give a legitimate distribution if $A_{51} = 2$. One finds that the weight distribution must be:

$i = 0$	33	36	42
$A_i = 1$	190	32	20

with the values not shown being 0.

We consider $C' = \mathrm{res}(C, a)$, with $w(a) = 42$, a [9, 4, 5] Griesmer code. Lemma 12 implies $B_1(C') = B_2(C') = B_3(C') = 0$, and Lemma 10 implies $A_9(C') = 0$ or 2. Once again, the MacWilliams identities allow only one legitimate distribution:

$i = 0$	5	6	7	8	9
$A_i(C') = 1$	36	24	0	18	2

Then we consider values of $w(\mathrm{res}(b, a))$ for $b \notin \langle a \rangle$, using Lemma 9. We find

$$3w(\mathrm{res}(b, a)) + 84 = w(b) + w(a + b) + w(2a + b).$$

Apart from order, the only sum on the right for $w(\mathrm{res}(b, a)) = 9$ is

$$111 = 42 + 36 + 33.$$

Thus the two 9's in C' require two 42's outside $\langle a \rangle$. As $\langle a \rangle$ also contains two 42's, there are 16 42's not producing 9's in C'. The lowest sum involving a 42 is $42+33+33=108=3\cdot 8+84$. So these 16 42's produce 8's in C'. That leaves two 8's, and the sum for them must be $108=36+36+36$.

What this means is that each word a with $w(a)=42$ is in a unique 2-dimensional subcode of C in which the six words outside $\langle a \rangle$ all have weight 36. Suppose $w(b)=36$ and b shows up in two such subcodes, corresponding to a and a' of weight 42 ($\langle a \rangle \neq \langle a' \rangle$). Then in Lemma 3 applied to $\langle a, a', b \rangle$, the weight count is at least

$$4\cdot 42+10\cdot 36+12\cdot 33=924.$$

But $3^{3-1}\cdot 2\cdot n(\langle a, a', b\rangle)\leqslant 18\cdot 51=918$, and there can be no such b. Thus we have 10 disjoint sets of six 36's, and that is incompatible with $A_{36}=32$.

This theorem was used by van Eupen, Hamada, and Watamori [10] to show that there is no [50, 5, 32] Griesmer code over $GF(3)$. They did that by showing that if there were, it would be obtained by puncturing a [51, 5, 33] code. Such an argument cannot usually be carried out (but a general setting was presented in [15]). In the divisible case, given the choice, one would rather show that the Griesmer code exists than show it does not! For if the parameters in question are, say, $[n, k, d]$ over $GF(p)$, with $n=g_p(k, d)$ and $p \mid d$, then $g_p(k, d-r)=n-r$ for $r<p$. Thus one could puncture an $[n, k, d]$ code repeatedly and obtain Griesmer codes for the minimum weights $d-r$, $r<p$. But $g_p(k, d+1)\geqslant n+2$ if $k\geqslant 2$, and existence at $d+1$ cannot be used with puncturing to get contradictory existence at d.

The third example illustrates trying to find "generic" Griesmer codes—codes constructed in a manner independent of the field. The geometric approach to Griesmer codes taken by Hamada and others (whose work is also surveyed in [14]) can be viewed in this light.

Consider the parameters $n=g_p(4, d)$, $k=4$, and $d=p^2+rp$ for Griesmer codes over $GF(p)$, p a prime, with $0<r<p-3$. We have $g_p(4, d)=p^2+(r+1)\,p+r+3$ (whence the upper bound on r). Thus by Theorem 1, if the Griesmer code exists, the possible nonzero weights are p^2+rp and $p^2+(r+1)\,p$.

Since $d\leqslant p^{4+1-2}$, $B_1=B_2=0$. The three equations from the MacWilliams identities (for $m=0, 1, 2$) are overdetermined, and there is a solution only if $r=(p-3)/2$. Taking that value, we have $n=3(p^2+1)/2$ and weights $d=3p(p-1)/2$, $d+p=(3p-1)\,p/2$. The weight distribution is

$$A_d=(p^2+1)(2p-1)(p-1)/2,$$
$$A_{d+p}=3(p^2+1)(p-1)/2=n(p-1),$$
$$B_3=(p^2+1)(5p+1)(p-1)^2/16.$$

This code has a dual in the two-weight code sense ([13], Theorem 8.7) having the same parameters. The Assmus–Mattson theorem [1, Theorem 4.2] applies and gives 1-designs. In fact, let $\mathscr{A}$ be the set of complements of the supports of words of weight $d+p$; these complements have size $(p+3)/2$. Let $\mathscr{B}$ be the set of supports of words of weight 3 in the dual. Then $\mathscr{A} \cup \mathscr{B}$ forms the block set for a partially balanced incomplete block design with $\lambda = 1$.

Do such codes exist? They do for $p = 5$, as recorded in [4]. A code for $p = 5$ also arises in recent constructions for difference sets by van Eupen and Tonchev [11] and Wilson and Xiang [23]. But the author is unaware of any generalization.

ACKNOWLEDGMENTS

Thanks are due to Ray Hill for much useful information and to Gary McGuire for helpful suggestions. Thanks also go to a referee who supplied a number of additional references.

REFERENCES

1. E. F. Assmus, Jr. and H. F. Mattson, Jr., New 5-designs, *J. Combin. Theory* **6** (1969), 122–151.
2. L. D. Baumert and R. J. McEliece, A note on the Griesmer bound, *IEEE Trans. Inform. Theory* **19** (1973), 134–135.
3. A. Bonisoli, Every equidistant linear code is a sequence of dual Hamming codes, *Ars Combinatoria* **18** (1983), 181–186.
4. I. Boukliev, S. Kapralov, T. Maruta, and M. Fukui, Optimal linear codes of dimension 4 over F_5, *IEEE Trans. Inform. Theory* **43** (1997), 308–313.
5. A. E. Brouwer and M. van Eupen, The correspondence between projective codes and 2-weight codes, *Des. Codes Cryptogr.* **11** (1997), 261–266.
6. S. M. Dodunekov, Minimum block length of a linear q-ary code with specified dimension and code distance, *Problems Inform. Transmission* **20** (1984), 239–249.
7. S. M. Dodunekov, "Optimal Linear Codes," Doctor of Math. Sciences Thesis, Institute of Mathematics, Sofia, Bulgaria, 1985.
8. S. M. Dodunekov, A comment on the weight structure of generator matrices of linear codes, *Problems Inform. Transmission* **26** (1990), 173–176.
9. S. M. Dodunekov and N. L. Manev, Minimum possible block length of a linear code for some distance, *Problems Inform. Transmission* **20** (1984), 8–14.
10. M. van Eupen, N. Hamada, and Y. Watamori, The nonexistence of ternary [50, 5, 32] codes, *Des. Codes Cryptogr.* **7** (1996), 235–237.
11. M. van Eupen and V. D. Tonchev, Linear codes and the existence of a reversible Hadamard difference set in $Z_2 \times Z_2 \times Z_5^4$, *J. Combin. Theory Ser. A* **79** (1997), 161–167.
12. N. Hamada, T. Helleseth, and Ø. Ytrehus, The nonexistence of [51, 5, 33; 3]-codes, *Ars Combinatoria* **35** (1993), 25–32.
13. R. Hill, Caps and codes, *Discrete Math.* **22** (1978), 111–137.

14. R. Hill, Optimal linear codes, *in* "Proceedings 2nd IMA Conference on Cryptography and Coding" (C. Mitchell, Ed.), pp. 75–104, Oxford Univ. Press, Oxford, 1992.
15. R. Hill and P. Lizak, Extensions of linear codes, "Proc. IEEE International Symp. Inf. Theory," Whistler, BC, 1995, p. 345.
16. R. Hill and D. E. Newton, Optimal ternary linear codes, *Des. Codes Cryptogr.* **2** (1992), 137–157.
17. I. Landgev, Nonexistence of some ternary five-dimensional codes, *Des. Codes Cryptogr.*, to appear.
18. F. J. MacWilliams, A theorem on the distribution of weights in a systematic code, *Bell System Tech. J.* **42** (1963), 79–94.
19. W. W. Peterson and E. J. Weldon, Jr., "Error-Correcting Codes," 2nd ed., MIT Press, Cambridge, MA, 1972.
20. H. N. Ward, Divisible codes, *Arch. Math. (Basel)* **36** (1981), 485–494.
21. H. N. Ward, Weight polarization and divisibility, *Discrete Math.* **83** (1990), 315–326.
22. H. N. Ward and J. Wood, Characters and the equivalence of codes, *J. Combin. Theory Ser. A* **73** (1996), 348–352.
23. R. M. Wilson and Q. Xiang, Constructions of Hadamard difference sets, *J. Combin. Theory Ser. A* **77** (1997), 148–160.